

Published and Copyright (c) 1999 - 2014
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

<http://people.delphiforums.com/dpj/a-one.htm>
Now available:
<http://www.atarinews.org>

Visit the Atari Advantage Forum on Delphi!
<http://forums.delphiforums.com/atari/>

==~==~==

~ Google Glass On Ropes? ~ People Are Talking! ~ Atari Dig on Hold?
~ Facebook Fights Back! ~ AT&T Rebuffs Netflix! ~ Cyber-gang Problem?
~ Gmail Scanning Case! ~ PS 4 Project Morpheus! ~ Google Drive Scam!

~ Dual-OS Tablets Halted ~ Internet Freedom Wanted ~ Feds Not Worried!

- * Turkey Blocks Twitter Access *-
- * Abandoning Internet, Obama Says No! *-
- * Google Makes It Harder To Spy on Your Gmail *-

==~==~==

->From the Editor's Keyboard
"~~~~~"

"Saying it like it is!"

Another week, another bout of time being a luxury that doesn't appear to be something I've found lately. There are just too many things going on that take priority. So, rather than try to comment of any number of interesting topics from around the globe, let's just move straight to another interest-laden issue!

Until next time...

==~==~==

->In This Week's Gaming Section
"~~~~~"

- Sony Reveals Project Morpheus!
- Walmart Will Accept Video Game Trade-Ins!
- Search For Old Atari Games To Go On in New Mexico!

xico!

And more!

==~==~==

->A-ONE's Game Console Industry News
"~~~~~"

- The Latest Gaming News!

Sony Reveals Project Morpheus, Its VR Headset for PlayStation 4

Sony has revealed its plans for virtual reality technology on the PlayStation 4. Shuhei Yoshida, president of Sony Worldwide Studios, showed off a prototype headset at a Game Developers Conference 2014 event entitled Driving the Future of Innovation. "Nothing delivers a feeling of immersion better than VR," said Yoshida. "VR has been a dream of many gamers since the computer was invented. Many of us at PlayStation have dreamed of VR and what it could mean to the gaming community."

The VR system is currently codenamed Project Morpheus, and will work with

PlayStation 4. While still in prototype form, Yoshida says that Morpheus is the "culmination of our work over the last three years to realize our vision of VR for games, and to push the boundaries of play." The headset uses a 1080p LCD, offers a 90-degree field of view, and will integrate with the PlayStation Camera for tracking and PlayStation Move for motion control. It connects via HDMI and USB; while the current prototype uses a 5-meter cable, Sony would like to make it wireless. The company says the headset doesn't put weight on your nose or cheeks, and its design allows for airflow without the lenses fogging up.

Sony Magic Lab's Richard Marks, who pioneered the EyeToy camera and PlayStation Move, joined Yoshida on stage to offer further details on Project Morpheus. "The thing that makes VR special is really the feeling of being in another place... there's no way to explain it to you that will make sense, but it's that feeling of presence," he said. "VR is going to be pervasive, and what I mean by that is it's going to be used for all sorts of things you might not think it would be used for." As one example, Marks says he's been working on a project with NASA and its Jet Propulsion Lab that will allow PS4 owners to feel like they're right with the space agency on Mars.

Marks has identified six areas that Sony needs to crack in order for VR to work: sight, sound, tracking, control, ease of use, and content. For sight, Marks refers to Sony's considerable weight in optics and imaging technology. For sound, the company is working on 3D binaural tech to aid presence and immersion. For tracking and control, Marks says the PlayStation Camera and PlayStation Move are ready-made solutions. For ease of use, Sony plans to make it a comfortable, plug-and-play experience. And for content, Marks showed a long list of software partners including Epic Games, Crytek, Autodesk, Unity, and more. Sony will be showing demos of Thief, EVE Valkyrie, and more running on Project Morpheus at GDC.

Although VR is yet to turn up a viable consumer product, the concept has been gaining momentum ever since Kickstarter-funded startup Oculus VR showed off its first headset, the Rift, in 2012. The company demonstrated a more refined Oculus Rift prototype, codenamed Crystal Cove, earlier this year, with more contenders set to join the fray. Valve is working on similar VR technology of its own, and Microsoft has explored augmented reality glasses, known as Project Fortaleza, that would work with the Xbox One's Kinect sensor.

Sony's announcement today, however, marks the first serious effort from a first-party platform holder, and could prove the most attractive option yet for VR developers. "We have seen passionate people at Oculus VR and Valve introduce VR prototypes and share their learnings," said Yoshida. "I have an enormous amount of respect for them. This shows how all of us as an industry can rally around a new medium like VR to push gaming forward." No release date is set for Project Morpheus, but Sony plans to make an SDK available to developers in the near future.

Update: Sony has confirmed to The Verge that Project Morpheus will not be made into a consumer product this year. The company isn't yet revealing when a finished product will arrive. The prototype shown at Game Developers Conference will be used to help familiarize Sony's developer partners with the VR technology.

Not wanting to let other retailers like GameStop, Best Buy, and Amazon have all the fun, Walmart has decided to enter the \$2 billion pre-owned video game business.

Walmart will allow for trade-ins to Walmart employees starting today, with official trade-ins to customers beginning on March 26th at over 3,100 stores. Then, in the Summer, Walmart will be reselling the used games in stores and online, calling them Certified Pre-Owned .

Walmart made sure to note that new releases will still remain the focus of our business, but when it comes to trading in games for a Walmart gift card (which can be used to buy anything in stores and online), their strategy is to pay more for used games, sell new and used games for less, and give our customers the flexibility to spend their money how they want. They also added, When we disrupt markets and compete, our customer wins.

$$= \sim = \sim = \sim =$$

```
->A-ONE Gaming Online      -      Online Users Growl & Purr!
   " " " " " " " " " " " "
```

Not So Fast: Environmental Concerns Halt Atari 'E.T.' Cartridge Dig

Filmmakers planned to excavate millions of the cartridges, buried as part of Atari's "corporate shame," but New Mexico regulators say an environmental report is required first.

An original E.T. game cartridge, signed by the lead designer. Millions were made, and most of them were buried in a New Mexico landfill after the game was deemed one of the worst ever.

New Mexico environmental regulators have put the kibosh on the excavation of millions of Atari "E.T." game cartridges from a garbage dump there.

According to The Guardian, the New Mexico Environment Department has said that filmmakers planning a documentary about the burial of the cartridges in 1983 owing to catastrophic sales must first acquire a waste excavation plan.

At South by Southwest earlier this month, filmmakers from Lightbox and Fuel Entertainment said they were almost ready to start digging into the garbage dump in Alamogordo, N.M., to look for the cartridges. Their research had led them there, they said, and they were planning on a long dig, since they didn't know precisely where in the dump the millions of games might be found.

Atari's E.T. game is universally considered one of the worst in history, brought to market in just weeks following the monumental success of Steven Spielberg's 1983 film "E.T." It was thought to be boring, aesthetically ugly, and shallow. Though it immediately sold 1.5 million

copies thanks to its ties to the movie, sales quickly stalled, and the result was a \$500 million loss for Atari, a financial disaster that drove the once high-flying company into ruin.

The episode has been referred to as Atari's "corporate shame."

Last June, the Guardian reported, city officials in Alamogordo approved the excavation. But New Mexico Environment Department spokesperson Jim Winchester told the publication that state environmental officials, who have the final say on the approval of a waste excavation plan, rejected it last month. He added that the filmmakers have yet to submit a new plan.

Requests for comment by CNET to the New Mexico Environment Department and Fuel Entertainment were not immediately returned.

Search For Old Atari Games To Go On in New Mexico

Organizers say a planned dig into a New Mexico landfill for a rumored cache of what some consider the worst Atari video game of all time is expected to proceed despite state environmental regulators' concerns.

Fuel Entertainment and LightBox Interactive are seeking to excavate an old Alamogordo landfill that reportedly was a dumping ground for "E.T. the Extra-Terrestrial" game cartridges.

Jonathan Chinn, an executive producer at Los Angeles-based LightBox, said Thursday that the search hasn't been halted.

Chinn says a local waste-management consultant who filed an excavation permit is addressing questions raised by the New Mexico Environmental Department.

A department spokesman has said the agency was waiting on a revised waste excavation plan.

"E.T." the video game, inspired by the hit 1982 movie, is said to have contributed to Atari's decline.

==~==~==

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

No, The U.S. Isn't Really Giving Up the Internet It Doesn't Own It Anyway

The United States National Telecommunications and Information Administration announced Friday evening that it would hand over its limited oversight of the Internet's domain-name system to an undefined,

new decision-making process.

Clearly, then, we're giving up on U.S. oversight of the Internet, and our government is hiding the fact by making the announcement on a Friday night.

If there's a 5:00 on Friday news dump, you'd better be concerned. Keep the Internet! tweeted former Republican Rep. Mary Bono. She had company in that assessment, as a variety of other GOPers denounced the proposal.

The idea of surrendering American control over one of the best things ever made in America isn't something to take lightly. Taken to an extreme, it suggests we've jacked into a future where Vladimir Putin deletes the registration for usa.gov (presumably while being whisked somewhere in a black helicopter).

But, surprise, last Friday's announcement doesn't mean that. It's not even new.

The U.S. began moving in this direction back in 1997, then reaffirmed it in 1998 when it transferred domain-name management duties to a Los Angeles based nonprofit called the Internet Corporation for Assigned Names and Numbers.

Ever since, it's been ICANN calling the shots over the machinery that assigns domain names like yahoo.com. It's also ICANN that decides whether to create new top-level domains such as .biz, .info, and maybe someday .sucks.

The government's remaining responsibility has essentially been OK'ing ICANN's proposed changes to the root zone of the domain name system the beating heart of the mechanism that routes Internet requests for particular site names that humans can read to numerical Internet Protocol addresses like 206.190.36.45, which computers understand.

Our role has always been a clerical, administrative role to make sure the system worked, said an NTIA official Monday afternoon.

In 2006, the government confirmed once again its intention to hand over that role to the global Internet community.

Friday's news amounts to the feds saying, The last two administrations weren't kidding. We still mean it.

So what has changed to make this news look so loaded in some quarters?

Some blame goes to the absurd level of inter-party hostility in Washington, and in particular the if the Obama administration wants this, it must be wrong school of thinking. But responsibility can be found all around Washington.

Foolish, failed attempts to rewrite the Internet's core code to stop pornography (the Communications Decency Act) and copyright infringement (the Stop Online Piracy Act) were bipartisan offenses. The NSA's bulk surveillance and efforts to weaken Internet-security standards also had support in both parties.

All those things seem to have led to a general suspicion of any government-instigated change to the Internet even if that change is to reduce government's role in the Internet.

And then something called WCIT happened. At the 12th annual World conference on International Telecommunications in Dubai two Decembers ago, other countries teamed up with the International Telecommunications Union to try to place Internet governance under that United Nations body.

The U.S. and like-minded countries balked at that and finally walked out of WCIT. Friday's announcement from the NTIA included this pointed deal-breaker: NTIA will not accept a proposal that replaces the NTIA role with a government-led or an inter-governmental organization solution.

What next, instead? That's an outstanding question.

The idea is to turn supervision of ICANN over to a multi-stakeholder process involving the Internet community worldwide that must keep the Internet secure, stable, resilient, and open. In tech-policy circles, the phrase multi-stakeholder process can translate to *mañana* or when I get around to it, but NTIA's current contract with ICANN runs out in September 2015.

If all goes well seriously, don't ask me how we get there from here the domain-name system will look and work about as it does now, but without crucial sign-offs coming from a Washington, D.C., address.

And that alone will count for something on a symbolic level. Other countries have never particularly liked the sense that the U.S. government had a privileged position relating to Internet governance, wrote Wendy Seltzer, policy counsel for the World Wide Web Consortium.

Christian Dawson, chairman of the Internet Infrastructure Coalition, made the same point: All this will really mean is different oversight for the same task oversight that better reflects the global Internet community.

But on a philosophical level, reinforcing that the Internet functions beyond any one .gov's control a step toward a world in which governments no longer assert oversight over the technology of communication, as George Mason University Mercatus Center scholar Eli Dourado wrote Monday would promote a longstanding libertarian aspiration.

That would be a remarkable accomplishment by this Democratic administration. Will it get any credit for that?

Obama Administration Denies 'Abandoning the Internet'

A top Commerce Department official pushed back Wednesday against concerns that the Obama administration is opening the door to an Internet takeover by Russia, China, and other authoritarian regimes.

The fears stem from the Commerce Department's announcement last Friday that it plans to give the Internet Corporation for Assigned Names and Numbers, an international nonprofit group, control over the technical system that allows computers to connect to Web addresses.

"Our announcement has led to some misunderstanding about our plan, with some individuals raising concern that the U.S. government is abandoning

the Internet. Nothing could be further from the truth," Lawrence Strickling, the assistant Commerce secretary for communications and information, said in a statement. "This announcement in no way diminishes our commitment to preserving the Internet as an engine for economic growth and innovation."

He said the U.S. government will continue to push ICANN to adopt policies that are in the interest of the United States and an open Internet.

The transition to full ICANN control of the Internet's address system won't happen until October 2015, and even then, there likely won't be any sudden changes. ICANN was already managing the system under a contract from the Commerce Department.

But having the ultimate authority over the domain-name system was the most important leverage the United States had in debates over the operation of the Internet. It was a trump card the U.S. could play if it wanted to veto an ICANN decision or fend off an international attack on Internet freedom.

Some have expressed concern that giving up that leverage could allow authoritarian governments or the United Nations to pressure ICANN to censor online content. For example, Rep. Marsha Blackburn, a Tennessee Republican, called the administration's announcement a "hostile step" against free speech.

"Giving up control of ICANN will allow countries like China and Russia that don't place the same value in freedom of speech to better define how the Internet looks and operates," she said in a statement on Monday.

The House Energy and Commerce Committee will hold a hearing on the plan next month and has promised "aggressive oversight." In a joint statement, Committee Chairman Fred Upton and Technology Subcommittee Chairman Greg Walden said that any changes to Internet governance should "be approached with a cautious and careful eye."

But Strickling noted that the National Telecommunications and Information Administration, a Commerce Department agency that he heads, will need to sign off on ICANN's proposal for managing the Internet address system.

"We have been clear throughout this process that any transition plan must meet the conditions of supporting the multistakeholder process and protecting the security, stability and resiliency of the Internet," Strickling said. "I have emphasized that we will not accept a proposal that replaces NTIA's role with a government-led or an intergovernmental solution. Until the community comes together on a proposal that meets these conditions, we will continue to perform our current stewardship role."

Strickling also pointed to supportive statements from Democrats including Senate Commerce Committee Chairman Jay Rockefeller and Rep. Anna Eshoo, as well as Republican Sens. Marco Rubio and John Thune. AT&T, Verizon, Cisco, Microsoft, and Google have also endorsed the move.

The U.S. government has long supported the "multistakeholder" model for Internet governance in which businesses, advocacy groups, and governments come together to make decisions. But because the Internet was invented in the United States, this country has historically had a central role in its management. As the Internet has grown, other countries have demanded a greater voice in decision-making. Edward Snowden's leaks about U.S.

surveillance have only intensified the international pressure on the United States to relinquish its power.

Facebook Fights Back Against the NSA Spy Machine

Mark Zuckerberg was apparently peeved enough to phone the president when he read recent reports that the NSA was using fake Facebook websites to intercept the social network's traffic and infect private computers with surveillance software. But Joe Sullivan the ex-federal prosecutor who now serves as Facebook's chief security officer said the company has now steeled its online services so that such a ploy is no longer possible.

That particular attack is not viable, the 45-year-old Sullivan told a room full of reporters yesterday at Facebook headquarters in Menlo Park, Calif. It hasn't been viable, he explained, since the company rolled out what's called SSL data encryption for all its web traffic, a process it completed in the summer of last year.

According to outside security researchers, there are still ways of working around Facebook's encryption. But these methods are much harder to pull off, and Sullivan's message was clear: The situation around the NSA's surveillance campaigns isn't quite as dire as many have painted it. Unlike his counterparts at places like Google and Microsoft, Sullivan said the revelations from NSA whistleblower Edward Snowden aren't really that surprising, and he indicated that the leaked information has changed little about how his company approaches security.

Sullivan's message stands in contrast to the one Zuckerberg unloaded on his Facebook page after phoning the president. The Facebook founder expressed extreme frustration over the NSA's practices, calling for sweeping changes to government policies. But the contrast isn't that surprising. It very clearly shows the awkward situation that has engulfed companies like Facebook in the wake of Snowden's revelations, which started tumbling out last summer. The giants of the web are certainly concerned over NSA surveillance despite indications that they may have been complicit in some ways and they're actively fighting against it. But they must also reassure customers that the situation is well in hand that it's safe to use their services today. This can be a difficult line to walk.

Certainly, the web's largest operations including Google, Yahoo, and Microsoft, as well as Facebook have now taken at least the basic steps needed to guard their online traffic against interlopers. Facebook not only uses SSL, or Secure Sockets Layer, encryption to protect all data moving between its computer servers and virtually all of the more than 1.2 billion people who use the social networking service, but it has also installed technology that uses similarly hefty encryption techniques to protect information that flows between the massive data centers that underpin its online empire. This is just the sort of thing Snowden himself called for last week while appearing via video feed at a conference in Texas.

In using SSL to encode all data sent and received by its millions of members, Facebook can indeed thwart the sort of fake-Facebook-server attack discussed in the press last week. As described, these attacks

redirected people to NSA websites that looked exactly like Facebook by surreptitiously slipping certain Internet addresses into their browsers. SSL encryption provides what is probably solid protection against such methods, said Nicholas Weaver, a staff researcher who specializes in network security at the International Computer Science Institute.

Weaver does acknowledge that attackers could compromise Facebook SSL encryption by somehow obtaining or creating fake encryption certificates, but he believes that such attacks are now unlikely. That is very risky these days, he said, pointing out that many companies are now on the lookout for such fake certificates.

It's equally important that Facebook is now encrypting information as it moves between data centers. Documents released by Snowden have shown that the NSA has ways of tapping lines that connect the massive computing centers operated by the likes of Google and Facebook. Sullivan declined to say when Facebook had secured these lines, but he's now confident that this makes it much more difficult for agencies like the NSA to eavesdrop on Facebook data as it travels through network service providers outside of the company's control. And Weaver agrees. Assuming that the company's encryption devices aren't sabotaged, he said, the data is secure as it travels across the wire. You'd need to break into the data center computers or the encryption devices themselves to access that data, he said.

But Sullivan's rather sunny view of Facebook security doesn't tell the whole story. Much of the rest of the web has yet to adopt similar encryption techniques, and there's still so much we don't know about what the NSA is capable of. It's also worth noting that Facebook's chief security officer sidestepped questions about future threats to the company's operation, including the possibility of a quantum computer that could break current encryption techniques. In the post-Snowden age, the giants of the web have certainly increased their security efforts. But there is always more to do.

Google Just Made It Harder For People (Cough Cough the NSA) to Spy on Your Gmail

Google has enhanced the encryption technology for its flagship email service in ways that will make it harder for the National Security Agency to intercept messages moving among the company's worldwide data centers.

Among the most extraordinary disclosures in documents leaked by former NSA systems analyst Edward Snowden were reports that the NSA had secretly tapped into the main communications links that connect Yahoo and Google data centers around the world.

Google, whose executive chairman, Eric Schmidt, said in November that he was outraged over the practice, didn't mention the NSA in Thursday's announcement, except in a veiled reference to last summer's revelations. The change affects more than 425 million users of Google's Gmail service.

Yahoo has promised similar steps for its email service by this spring.

Google and other technology companies have been outspoken about the U.S. government's spy programs. The companies are worried more people will

reduce their online activities if they believe almost everything they do is being monitored by the government. A decline in Internet use could hurt the companies financially by giving them fewer opportunities to show online ads and sell other services.

"Your email is important to you, and making sure it stays safe and always available is important to us," Nicolas Lidzborski, Gmail's security engineering lead, wrote in a blog post.

Lidzborski said that all Gmail messages a consumer sends or receives are now encrypted.

"This ensures that your messages are safe not only when they move between you and Gmail's servers, but also as they move between Google's data centers something we made a top priority after last summer's revelations," Lidzborski wrote.

The NSA has said it only focuses on targets with foreign intelligence value.

A secret Jan. 9, 2013, accounting indicated that NSA sends millions of records every day from Yahoo and Google internal networks to data warehouses at the NSA's Fort Meade, Md., headquarters, according to documents released by Snowden and obtained by The Washington Post last year.

The NSA's principal tool to exploit the Google and Yahoo data links is a project called MUSCULAR, operated jointly with the agency's British counterpart, GCHQ. NSA and GCHQ are copying entire data flows across fiber-optic cables that carry information between the data centers of the Silicon Valley giants, the Post reported.

President Barack Obama has promised to consider changing some of the surveillance programs that Snowden disclosed. But the type of surveillance Google is trying to prevent by improving its encryption technology is not among the reforms Obama has discussed.

Google and other technology companies provide information to the NSA and other government agencies when required by a court order.

"Google is making it tougher for the government to spy on its customers without going through Google," said Chris Soghoian, a senior policy analyst at the American Civil Liberties Union.

"There are still ways for NSA to spy on the bad guys," Soghoian said. "But this will prevent them from spying on 500 million people at once."

Turkey Blocks Access to Twitter for Entire Country Days Before Major Election

Turkey's courts have blocked access to Twitter days before elections as Prime Minister Tayyip Erdogan battles a corruption scandal that has seen social media platforms awash with alleged evidence of government wrongdoing.

The ban came hours after a defiant Erdogan, on the campaign trail ahead of key March 30 local elections, vowed to wipe out Twitter and said he did not care what the international community had to say about it.

Erdogan's ruling AK Party has already tightened Internet controls, handed government more influence over the courts, and reassigned thousands of police and hundreds of prosecutors and judges as it fights a corruption scandal he has cast as a plot by political enemies to oust him.

Telecoms watchdog BTK said the social media platform had been blocked by the courts after complaints were made by citizens that it was breaching privacy. It said Twitter had ignored previous requests to remove content.

Because there was no other choice, access to Twitter was blocked in line with court decisions to avoid the possible future victimization of citizens, it said.

San Francisco based Twitter said it was looking into the matter but had not issued a formal statement. The company did publish a tweet addressed to Turkish members instructing them on how to continue tweeting via SMS text message.

Twitter, mwitter! Erdogan told thousands of supporters at a rally late on Thursday, in a phrase translating roughly as Twitter, schmitter!

We will wipe out all of these, said Erdogan, who has cast the corruption scandal as part of a smear campaign by his political enemies.

The international community can say this, can say that. I don't care at all. Everyone will see how powerful the Republic of Turkey is, he said in a characteristically unyielding tone.

Twitter members in Turkey began reporting widespread outages overnight. Some trying to open the Twitter.com website were taken to a statement apparently from another regulator (TIB) citing four court orders as the basis for the ban.

The corruption investigation became public on Dec. 17, when police detained the sons of three cabinet ministers and businessmen close to Erdogan. The three ministers resigned a week later, while others were removed in a cabinet reshuffle.

At an extraordinary session on Wednesday, Parliament's speaker blocked opposition pleas to have a prosecutor's report with allegations against the former ministers read out.

A document purporting to be that report appeared on Twitter last week. It included alleged transcripts of wiretapped phone conversations, pictures from physical surveillance, and pictures of official documents accusing the former ministers and two of their sons of involvement with an Iranian businessman in a bribery and smuggling racket.

Reuters has not been able to verify the authenticity of the document.

Turkish citizens were quick to come up with ways to circumvent the block. The hashtag #Twitterisblockedinturkey quickly moved among the top trending globally.

The disruption sparked a virtual uproar, with many comparing Turkey with Iran and North Korea, where social media platforms are tightly controlled.

There were also calls to take to the street to protest, although some equally called for calm.

Nazli Ilicak, a columnist who used to work for the pro-government Sabah newspaper described the move as a civil coup in an interview on broadcaster CNN Turk.

The move was only the latest clash between Turkey's ruling party and social media companies including Google, Facebook, and Twitter.

After a series of popular protests partly fueled by Twitter last summer, Erdogan slammed the service as a scourge.

Shortly thereafter, a government minister asked Twitter to establish an office in Turkey so that it could better communicate requests to take down content or hold the company accountable to Turkish law. Twitter did not respond to the request.

Erdogan said two weeks ago that Turkey could also ban Facebook and YouTube, which he says have been abused by his enemies after a stream of audio recordings purportedly revealing corruption in his inner circle emerged online.

But a senior official said on Friday there were no immediate plans to do so.

The path was taken to block access within the framework of a court decision because of the failure to overcome the problem with the management of Twitter, the official said.

At the moment there is no such a decision for Facebook and other social media, he told Reuters.

California Has a Cyber-Gang Problem

International criminal enterprises follow the money, and a report being released Thursday says they are increasingly focusing on California because of its wealth and innovation.

Aside from longtime trafficking in drugs, guns, and people, the report by California Attorney General Kamala Harris says criminals are turning to cybercrime to target businesses and financial institutions.

It calls California the top target in the United States for organizations that often operate from safe havens in Eastern Europe, Africa, and China.

California is a global leader on a number of fronts and, unfortunately, transnational criminal activity is one of them, the report states.

Harris said it is the first comprehensive report to outline the effects international criminal organizations are having on Californians and businesses in the state. She released a 181-page report during a late-morning news conference with other law enforcement officials in Los Angeles.

California leads all states in the number of computer systems hacked or infected by malware, the number of victims of Internet crimes, the amount of financial losses suffered as a result, and the number of victims of identity fraud. The report says the state also is particularly vulnerable

to thefts of intellectual property because of its leading role in developing new technologies and mass-media entertainment.

Not surprisingly, transnational organized crime has tapped into this new criminal frontier, the report says. Many of these breaches have been tied to transnational criminal organizations operating from Russia, Ukraine, Romania, Israel, Egypt, China, and Nigeria, among other places.

California's gross domestic product of \$2 trillion, significant foreign trade activity, and border with Mexico also make the state an easy target for international money-laundering schemes, the report says. It estimates that more than \$30 billion is laundered through California's economy each year.

Some is filtered through legitimate businesses or by using virtual currencies such as Bitcoin. But the report says backpacks and duffel bags stuffed with cash have been seized more frequently since Mexico began toughening its money-laundering laws in 2010.

Seizures of bulk cash increased 40 percent by 2011 in California, which now leads the nation in the number of currency seizures.

California should alter state law to make it easier for prosecutors to crack down on money laundering, the report says. Unlike federal law, state law currently requires prosecutors to prove that a suspect deliberately carried out a financial transaction in a way designed to hide the fact that the money came from or was used for a criminal activity.

The report also recommends that the Legislature change state law to let prosecutors temporarily freeze the assets of transnational criminal organizations and associated gangs before they seek an indictment.

It also calls for the state to devote more money to the state Department of Justice, which Harris leads. That would include \$7.5 million to fund five new teams that would target international criminals.

Beware of This Google Drive Scam Stealing Your Info

Usually, you can tell a legitimate Google notification from a phishing scam by reading the URL's domain name: a message that redirects you to a non-Google address is sure to be a scam. However, a sophisticated phisher has come up with a method of stealing Google login information by using the company's own servers against it.

Sunnyvale, Calif.-based security firm Symantec discovered the phishing attempt and reported the incident on its blog. The scam comes in an email titled "Documents" and encourages you to click on an included link to check out an important message on Google Drive.

This link leads to a login page hosted on a bona fide Google URL, complete with Secure Sockets Layer (SSL) authentication. The login prompt is identical to that of a real Google site, inviting you to sign in for "One account. All of Google." Those who log in get access to a Google Drive document that says nothing of great import.

Of course, the document isn't the point; the point is that the phishers

now have access to your Google account. This gives them access to Google Drive documents, private email, and perhaps most damning payment information for Google Play.

The trick works because the lure document is actually hosted on Google Drive. Combined with the convincing login page, this trick could theoretically fool the tech savvy as well as the uninformed.

Still, cautious people would spot a few red flags in this otherwise clever scam. First of all, the email itself does not come from an official Google email address, even if its preferred display name indicates otherwise. Clicking on links embedded in emails is also generally a bad practice, although in this case, even copying and pasting it would still bring you to a verified Google page.

If you get an email message purporting to come from a big organization such as Google, it's generally a good idea to check the content of the email against the company's official blog or Twitter feed. A company will rarely institute policy changes without informing you on a grand scale.

Don't feel too bad if you got taken in by this one, but do change your password as soon as possible, and consider implementing two-step authentication for your Google account.

Judge Rejects Class-Action Bid in Gmail-Scanning Case

Google scored a victory this week in a long-running Gmail lawsuit when a California judge denied a request to turn it into a class-action suit.

As a result, plaintiffs will be forced to pursue the case separately, a costly move that might not have a lucrative enough outcome to make it a worthwhile endeavor.

At issue is a feature within Gmail that anonymously scans the contents of peoples' emails to serve up targeted ads on the right-hand side of the inbox. The lawsuit claims the practice violates federal and state wiretap laws, but Google has long held that scanning is done via an algorithm; no humans at Google are reading peoples' emails.

In September, Judge Lucy Koh rejected Google's request for dismissal after the search giant argued that "just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use Web-based email today cannot be surprised if their communications are processed by the recipient's ECS [electronic communications service] provider in the course of delivery." But Judge Koh found that the scanning of emails is not considered an "instrumental part of the transmission of email."

Today, however, Judge Koh focused on whether the plaintiffs consented to the alleged interceptions within Gmail. In this case, she found, the consent issues are too different to combine into a class action.

"Specifically, there is a panoply of sources from which email users could have learned of Google's interceptions other than Google's TOS and Privacy Policies," she wrote, pointing to Google-crafted websites, as well as media reports.

"Some Class members likely viewed some of these Google and non-Google disclosures, but others likely did not," she continued. "A fact-finder, in determining whether Class members impliedly consented, would have to evaluate to which of the various sources each individual user had been exposed and whether each individual 'knew about and consented to the interception' based on the sources to which she was exposed."

Ultimately, that would "lead to numerous individualized inquiries that will overwhelm any common questions," the judge concluded.

AT&T Rebuffs Netflix CEO's Net Neutrality Defense

It probably isn't often that AT&T and Verizon Wireless find themselves to be allies, but net neutrality might be one subject on which their interests align.

In direct response to a pointed memo by Netflix CEO Reed Hastings on Thursday, AT&T's public policy chief Jim Cicconi presented a rebuttal on Friday.

Much like Hastings, Cicconi doesn't mince words in defending the stance of the nation's second largest wireless provider, which essentially boils down to the somewhat rhetorical question that headlines the memo, "Who Should Pay for Netflix?"

Here's an excerpt:

As we all know, there is no free lunch, and there is also no cost-free delivery of streaming movies. Someone has to pay that cost. Mr. Hastings' arrogant proposition is that everyone else should pay but Netflix. That may be a nice deal if he can get it. But it is not how the Internet, or telecommunication for that matter, has ever worked.

To recall, Verizon Wireless won a court challenge to net neutrality rules, leading the U.S. Court of Appeals in Washington D.C. to send the rules back to the FCC in January.

This immediately sparked a debate about the future of the Internet as the move essentially means broadband companies would be able to charge tech companies, such as Netflix or Hulu, more money for fast connections needed to deliver their services.

It's up to the FCC now to rewrite the rules. In February, FCC chairman Tom Wheeler published a proposal he asserted will preserve the Internet as "an open platform for innovation and expression."

If there is one company that would benefit from the upholding of net neutrality, it is Netflix.

Microsoft and Google Ruin Intel's Plan for Dual-OS Tablets

Asus' dual-boot Transformer Book Duet is dead. At CES this year, one of the big stories was dual-OS devices. Spurred on by encouragement from chipmaker Intel, Asus announced the Transformer Book Duet, a hybrid

laptop and tablet that switches between Microsoft Windows and Google's Android on the fly. The device was an intriguing highlight at a trade show that was generally devoid of interesting laptops and tablets, and was scheduled for release in the US this month. Unfortunately, the device has likely been cancelled due to strong opposition from Microsoft and Google, according to a report from The Wall Street Journal.

Even before it was announced, the writing was on the wall for the Transformer Book Duet. "[Google and Microsoft] each have their sensitivities to this," one source told us in early January. With pressure mounting from both sides, Asus was forced to abandon the Duet, and, according to a leaked memo obtained by the WSJ, it will also stop selling a pair of dual-OS all-in-one PCs it launched last year.

A large reason for the halt of sales, says the memo, is Microsoft has a "new policy" of not supporting dual-OS products. Patrick Moorhead, principal analyst at Moor Insights and Strategy, told us in January that "Microsoft does not want [dual-OS devices] to happen," and now tells The Wall Street Journal that "Google wants all-Android devices" as well. It looks like the software giants got their way this time, and will now force hardware manufacturers and consumers to choose between Windows 8.1, Android, Windows RT, and Chrome OS for their upcoming devices.

Google Glass Is on the Ropes. Could be Finished

Google Glass has been an inspired product. Along the way, however, Google forgot one important thing: to create a thoughtful and beloved product, support it, and develop a considered path to market. That's why Glass looks to be history according to one of its strongest supporters, Robert Scoble.

When Paul Thurrott launched his straight talk about Windows 8, the fantasy was over for Microsoft. Mr. Thurrott exposed the fundamental weakness of the Windows 8 strategy. The product is now hopelessly damaged, and Microsoft will likely write it off as mistake, like Vista, and move on with Windows 9.

On March 19, Robert "Mister Google Glass" Scoble did the same thing to Google. The most notable fan of Google Glass, the ultimate glasshole, has bluntly exposed critical problems with Google's handling of the product.

Mr. Scoble, in a recent Google+ post sums it up:

Larry Page is on stage at TED right now. I'm at home watching. He is not wearing Google Glass.

This fits the new narrative that's going on in my head: that Google doesn't know how to stick with a product. Remember Google Wave? It was a very interesting idea, but Google gave up on it very quickly. Why? Because it was controversial and the execution wasn't good.

R. Scoble when he was in love with Google Glass in early 2013.

Suddenly the stark contrast between Google and Apple is brought into focus. Google has been highly praised lately for its aggressive introduction of technologies, but now we're seeing how a complete product strategy is lacking. Google throws cool technology against the wall to

see what sticks while Apple thinks deeply about solving fundamental human problems with the assistance technology. That takes more time.

Even Slate has created a holding spot for Google Glass in the Google Graveyard of products.

Because Google has had no well thought-out product strategy and because the technology has basically drifted for two years, Mr. Scoble observes: "Google Glass is a deeply flawed product [emphasis mine]. I wrote about how in my 'Glass is doomed' post."

Part of the problem has been that the social issues of Glass have proved too difficult to overcome. A person near others wearing Google Glass is irrationally ostracized. That's just the way it will be until the technology is so well miniaturized that it's no longer visible to others.

I've seen some last-gasp activity going on by tech writers. Mike Elgan, a fantastic observer and writer, has written what may turn out to be a brilliant epitaph for Google Glass. It boils down to a plea to be loved, yet left alone while in public with Glass, and it's oh-so poignant. "Am I a Glasshole? Or Are You a Self-Absorbed, Irrational Luddite?" The article tells us everything that's wrong about people, but also punctuates everything that's wrong with Glass at the same time.

In another last-gasp attempt to turn the product around, Google itself is trying to undo so many of the Glass myths that have evolved. "The Top 10 Google Glass Myths."

What have we learned? It's a mistake to conclude that because some company has rushed a futuristic product to market with lots of fanfare that Apple is doomed if it doesn't respond in kind right away. Apple's competitors have shown little interest in fundamentally changing the world with deep insights in to industrial design and human factors, and that's why they can toss products and services our way, scattergun, to see what sticks. Only the tech press panics, not Apple.

To put a gentle twist on it, photos of pretty women wearing Google Glass do not fully define a product or create a solid foundation for the product's future. The photos only mask the social reality with a fantasy. For those who have forgotten, we thank Apple every day for its deep insights into product design and its ability to then follow-through in the marketplace with a supported, growing, and eventually a beloved product like the iPod and iPad.

Apple doesn't try to do everything. It says "no!" to a lot of things when there's no fundamental human solution to be embraced. We've been reminded of the truth once again. Pay no attention to the wizards behind their curtains, flashing around their toys.

\$30K Worth of Multimeters Must Be Destroyed Because They're Yellow

An anonymous reader points out a post at the blog of Sparkfun, a hobbyist electronics retailer. They recently received a letter from U.S. Customs saying a shipment of 2,000 multimeters was being barred from entry into the country. The reason? Trademark law. A company named Fluke holds a trademark on multimeters that have a 'contrasting yellow border.' Sparkfun's multimeters are a yellowish orange, but it was enough for

Customs to stop the shipment. Returning the shipment is not an option because of import taxes in China, so the multimeters must now be destroyed. At \$15 per item, it'll cost Sparkfun \$30,000, plus the \$150/hr fee for destroying them. Sparkfun had no idea about the trademark, and doesn't mind changing the color, but they say restrictions like these are a flaw in the trademark system. "Small business does not have the resources to stay abreast of all trademarks for all the products they don't carry. If you're going to put the onus on the little guy to avoid infringing IP then you shouldn't need an army of consultants or attorneys to find this information."

Feds Aren't Worried About Windows XP Vulnerabilities

Federal agencies do not anticipate trouble when Microsoft early next month stops providing updated fixes for security flaws in the Windows XP operating system, top Obama administration officials say.

The Washington Post reported that about 10 percent of government computers, out of several million, will still be running XP when support ends on April 8. According to the newspaper, the problem is urgent, because vulnerabilities in the XP computers could allow intruders into larger networks.

But White House officials say they feel individual agencies are prepared for the expiration of XP support and don't see a need to take top-down action.

Agencies have made significant progress in moving off Windows XP, and the federal government is ahead of the private sector in this regard," a White House Office of Management and Budget official said. During conversations with agency personnel, "we have received no indication that agencies require any additional OMB intervention at this time."

Banks have been scrambling to upgrade the 2.2 million XP-based ATMs still using the 12-year-old operating system. According to Reuters, the cost of special deals with Microsoft for extended support or upgrades could be about \$100 million for each of Britain's main banks.

Some agencies have decided it is cheaper or more efficient to stick with XP. Typically, this is because their systems are not connected to the Internet where viruses spread - or are impossible to overhaul.

Agencies continuing to use XP "have put in place contingency plans to ensure that the risks associated with maintaining XP are mitigated," the OMB official said. "This is not an approach that is unique to the government - the private sector is approaching the migration in a similar way."

Administration officials could not tabulate the total cost of the changeover.

The Homeland Security Department, tasked with overseeing governmentwide cybersecurity, has been providing agencies with free "continuous diagnostics" tools to help pinpoint vulnerabilities in their systems. This aid should allow agencies to focus time and money on resolving the most significant weaknesses first, including the updating of software as necessary," DHS spokesman S.Y. Lee said.

"As a matter of law and policy, all agencies are responsible for the security of their networks and systems, and that includes addressing these known software vulnerabilities through ongoing patching," he said.

At Lee's own department, a switch to Windows 7 is expected to complete before April 8, according to DHS officials.

Microsoft's website states that, after April 8, XP users will stop receiving updates that "help protect your PC from harmful viruses, spyware, and other malicious software, which can steal your personal information. Also, the reliability of Windows might wane without the installation of new drivers for hardware and other tools, company officials said.

But Microsoft officials seem confident that federal customers will be shielded from hackers come April 9.

Because we are tightly working with our customers, and because of the types of systems that have yet to make the move off XP, we do not feel there is a substantially greater risk for the federal government on April 9 than there is on April 7, Mark Williams, Microsoft's chief security officer for federal systems, told The Post. That being said, at the end of the day, it's important to remember that the most safe system is a modern one.

Microsoft Office for iPad Will Be Unveiled This Month

Satya Nadella is planning to host his first press event as Microsoft CEO next week. The software maker has been inviting members of the media to a special cloud- and mobile-focused event in San Francisco on March 27th. Nadella is expected to discuss Microsoft's "mobile first, cloud first" strategy, and there will be some major news ahead of the company's Build conference in early April. Sources familiar with Microsoft's plans tell The Verge that the event will mark the introduction of Office for iPad.

Microsoft has been working on the software for a number of months now, having first introduced an iOS version of Office for the iPhone in June last year. We understand the iPad variant of Office will be similar to the iPhone version, and will require an Office 365 subscription for editing. We're told that document creation and editing is fully supported for Word, Excel, and PowerPoint apps. Overall, the interface and features are expected to be similar to the existing iPhone version.

Nadella's unveiling of Office for iPad will be the first major press event for the new CEO, but it will also underline his strategy for Microsoft. Nadella hinted at "cloud first, mobile first" shortly after he was named CEO last month, and Microsoft launched a Mac version of its OneNote Office app today, along with Office Online recently. The March 27th event will set the stage for further announcements at the Build developer conference on April 2nd. Microsoft will unveil Windows Phone 8.1 at Build, and the company is expected to fully detail its Windows 8.1 Update and hint at some future plans for Windows 9.

A censorship-free Internet is a priority for most people in emerging countries, especially the younger population, according to a new report.

Pew Research Center interviewed nearly 22,000 people in 24 emerging and developing countries between March and May for the report released Wednesday.

In 22 of those 24 countries, the majority of respondents think "it is important that people have access to the internet without government censorship." (Uganda just missed the cutoff, at 49 percent, and Pakistan was significantly lower at just 22 percent.)

The strength of censorship opposition varied by country, as well as other factors. Support of Internet freedom is prevalent in Latin American countries as well as Lebanon and Egypt, Pew said.

Unsurprisingly, anti-censorship sentiment tends to be strong in nations where Internet use is more common, such as Chile and Argentina. The trend is reversed in less connected nations like Uganda.

But two countries bucked that trend: Internet-freedom support in Russia (63 percent) and Pakistan (22 percent) came in low compared with the level of Internet penetration in those countries.

Age is also a major factor: In 14 of the 24 countries surveyed, people ages 18-29 are more likely than those 50 or older to think a free Internet is important. In nations including Russia and Lebanon, that age gap came in at 20 percentage points or more.

"These age differences suggest that support for internet freedom will only become more widespread with the passage of time," Pew said in its report.

==~==~==

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.